AMENDMENTS TO THE CLAIMS

Applicant submits below a complete listing of the current claims, including marked-up claims with insertions indicated by underlining and deletions indicated by strikeouts and/or double bracketing. This listing of claims replaces all prior versions, and listings, of claims in the application:

Listing of the Claims

1-20. (Canceled)

21. (Previously presented) A computer-implemented method, comprising:

receiving, by an interception module communicating with a firewall via a first application programming interface, via a second application programming interface at least one policy established by a first user that permits at least one of an application and a service to connect to a network when the first user runs the at least one of the application and a service, wherein the at least one policy is stored among a plurality of policies in a policy cache of the interception module;

receiving, by the interception module a connect attempt, a listen attempt, or a combination thereof from the application or the service run by a second user;

extracting, by the interception module, user and application or service information from the connect attempt, the listen attempt, or the combination thereof;

determining, by the interception module, an identity of the second user and what application or what service is making the connect attempt, the listen attempt, or the combination thereof;

determining, by the interception module, whether the identity of the second user matches an identity of a user that established the at least one policy and whether the connect attempt, the listen attempt, or the combination thereof comply with the at least one policy; and

when the connect attempt, the listen attempt, or the combination thereof comply with the at least one policy and the identity of the second user matches the identity of the user that established the at least one policy, instructing, by the interception module, the firewall to automatically create a configuration to allow the connect attempt, the listen attempt, or the combination thereof, and storing the configuration in a filter cache of the interception module.

22. (Previously presented) The method of claim 21, further comprising sending a notification to a user of a connect attempt, a listen attempt, or a combination thereof.

23. (Previously presented) The method of claim 22, wherein sending the notification comprises receiving a user input indicative of allowing a connection thereby creating the at least one policy.

24. (Previously presented) The method of claim 21, wherein establishing the at least one policy further comprises receiving a policy from the application or service.

25. (Previously presented) The method of claim 24, wherein receiving the policy comprises receiving the policy via an application programming interface.

26. (Previously presented) The method of claim 24, wherein the policy received from the application or service comprises inbound or outbound restrictions using one or more of Internet Protocol addresses, information about a subnet, information about scope of the connection, or combinations thereof.

27. (Original) The method of claim 24, wherein the policy received from the application or service comprises communication security level.

28. (Original) The method of claim 27, wherein the communication security level comprises authentication.

29. (Original) The method of claim 27, wherein the communication security level comprises encryption.

30. (Previously presented) The method of claim 21, wherein the firewall comprises a host firewall located on a computer comprising the application or the service.

31. (Original) The method of claim 21, wherein the firewall comprises an edge firewall, and further comprising an agent to communicate information about the connection.

32. (Original) The method of claim 21, wherein the firewall comprises an edge firewall, and further comprising an authenticated protocol to communicate information to the edge firewall about the connection.

33. (Previously presented) A computer-storage medium encoded with a computer program for performing the method recited in claim 21.

34-36. (Canceled)

37. (Previously presented) A computer system, comprising:

a firewall; and

an interception module communicating with the firewall via a first application programming interface, the interception module including a second application programming interface for establishing, by a first user, at least one policy that permits at least one of an application and a service to connect to a network when the first user runs the at least one of the application and a service, wherein the at least one policy is stored in a policy cache of the interception module, the interception module is configured and adapted to:

intercept a request for a connect attempt, a listen attempt, or a combination thereof from the application or the service run by a second user;

extract user and application or service information from the connect attempt, the listen attempt, or the combination thereof;

identify the user and the application or the service from the user and application or service information;

determine whether an identity of the second user matches an identity of a user that established the at least one policy and whether the connect attempt, the listen attempt, or the combination thereof comply with the at least one policy; and

when the connect attempt, the listen attempt, or the combination thereof comply with the at least one policy and the identity of the second user matches the identity of the user

that established the at least one policy, instructing the firewall to create a configuration to allow the connect attempt, the listen attempt, or the combination thereof, and storing the configuration in a filter cache of the interception module.

38. (Canceled)

39. (Previously presented) The computer system of claim 37, wherein the interception module comprises a firewall client for communicating information about the connect attempt, the listen attempt, or the combination thereof to an edge firewall.